

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-134229

(43) 公開日 平成10年(1998) 5月22日

(51) Int.Cl.⁶
G 0 7 D 9/00
G 0 6 F 17/60
19/00
G 0 6 T 7/00

識別記号
4 6 1

F I
G 0 7 D 9/00 4 6 1 A
G 0 6 F 15/21 3 4 0 B
15/30 3 3 0
3 4 0
15/62 4 6 0

審査請求 未請求 請求項の数5 F D (全 8 頁)

(21) 出願番号 特願平8-303843
(22) 出願日 平成8年(1996)10月30日

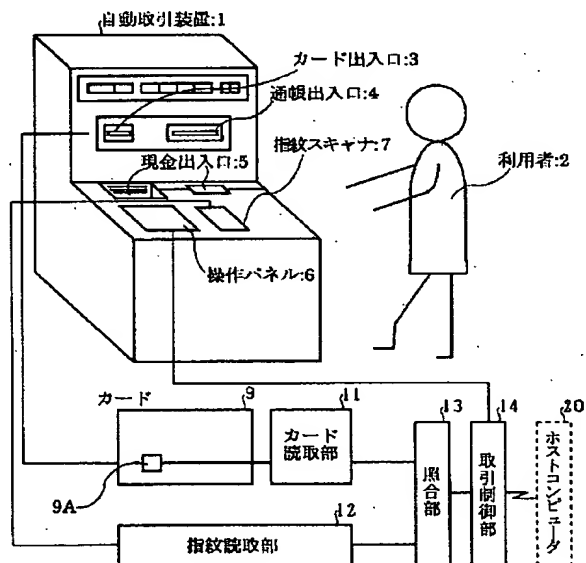
(71) 出願人 000000295
沖電気工業株式会社
東京都港区虎ノ門1丁目7番12号
(72) 発明者 西山 正
東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内
(72) 発明者 酢谷 昌史
東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内
(74) 代理人 弁理士 佐藤 幸男 (外1名)

(54) 【発明の名称】 自動取引装置及び自動取引システム

(57) 【要約】

【解決手段】 自動取引装置1には、指紋スキャナ7が設けられている。利用者2がカード9を投入すると、そこに格納された指紋データが読み出され、利用者2の指紋と照合される。こうしてカード所有者本人が操作していることを確認して取引を開始する。

【効果】 年金支給等、本人のみに取引を認める操作について、確実に本人確認を行うことができる。



具体例1のシステムのブロック図

【特許請求の範囲】

【請求項1】 利用者の指紋を読み取る指紋読取部と、利用者が投入したカードから指紋データを読み取るカード読取部と、前記指紋読取部の出力とカード読取部の出力とを照合して、前記利用者がカードの所有者本人であるかどうかを判定する照合部と、照合部の照合結果に基づいて、前記利用者による所定の取引を制御する取引制御部とを備えたことを特徴とする自動取引装置。

【請求項2】 利用者の指紋を読み取る指紋読取部と、利用者が入力した暗証コードと前記指紋読取部の出力とをホストコンピュータに送信する通信制御部と、ホストコンピュータ側において、予め登録された暗証コードと指紋データと、受信した暗証コード及び指紋読取部の出力とを照合して本人確認を実行する本人確認処理部とを設けたことを特徴とする自動取引システム。

【請求項3】 自動取引装置側において、利用者の指紋を読み取る指紋読取部と、利用者が投入したカードから、口座番号を読み取ってホストコンピュータに送信する通信制御部と、ホストコンピュータ側において、指紋データベースから前記口座番号に対応させて格納した指紋データを読み出して、利用者端末側に返送する指紋データベース検索部と、自動取引装置側において、返送された指紋データと、前記指紋読取部により読み取った指紋とを照合して、本人確認を行う照合部とを備えたことを特徴とする自動取引システム。

【請求項4】 請求項3において、通信制御部は、利用者が入力した暗証コードと取引データとをホストコンピュータに送信し、ホストコンピュータ側において、自動取引装置側で指紋照合の結果本人と確認されると、暗証コードを利用して更に本人確認を行うとともに、取引データを使用して取引を実行して自動取引装置側に通知する制御部を備えたことを特徴とする自動取引システム。

【請求項5】 自動取引装置側において、利用者の指紋を読み取る指紋読取部と、利用者が投入したカードから口座番号を読み取って、利用者が入力した暗証コードと共にホストコンピュータに送信する通信制御部と、ホストコンピュータ側において、前記暗証コードを利用して本人確認を行い、本人と判断されたとき、指紋データベースから前記口座番号に対応させて格納した指紋データを読み出して、利用者端末側に返送する指紋データベース検索部と、自動取引装置側において、

返送された指紋データと、前記指紋読取部により読み取った指紋とを照合して、本人確認を行う照合部とを備えたことを特徴とする自動取引システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、本人確認処理に指紋データを利用した自動取引装置及び自動取引システムに関する。

【0002】

10 【従来の技術】金融機関の窓口業務に対する負担軽減のために、顧客が操作する自動取引装置が広く普及している。この装置は、顧客が取引の種類を選択し、キャッシュカードや通帳等を投入することによって、その取引を自動的に実行する。こうした自動取引装置（ATM）は、銀行の預貯金取引のみならず、年金支給等の現金を取り扱う業務に広く利用されようとしている。従来、年金支給業務は、顧客が金融機関の窓口において、本人確認のための身分証明書を提出し、係員がその照合を行うといった手続がとられていた。

20 【0003】

【発明が解決しようとする課題】ところで、上記のような年金支給等の業務を自動取引装置を用いて行おうとすると次のような解決すべき課題が発生した。自動取引装置を用いて預金の引出しをする場合には、顧客はキャッシュカードを自動取引装置に投入して暗証コードを入力する。この暗証コードは、通常、4個程度の数字の組合せにより構成されており、必ずしも安全性の面で確実とはいえない。しかも、暗証コードを知っていれば本人以外の者でも操作が可能である。年金支給は原則として本人のみが受けることができるもので、自動取引装置に対し暗証コード等の入力のみならず、本人確認機能も付与することが必要になる。

【0004】

【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

〈構成1〉利用者の指紋を読み取る指紋読取部と、利用者が投入したカードから指紋データを読み取るカード読取部と、上記指紋読取部の出力とカード読取部の出力とを照合して、上記利用者がカードの所有者本人であるかどうかを判定する照合部と、照合部の照合結果に基づいて、上記利用者による所定の取引を制御する取引制御部とを備えたことを特徴とする自動取引装置。

40 【0005】〈構成2〉利用者の指紋を読み取る指紋読取部と、利用者が入力した暗証コードと上記指紋読取部の出力とをホストコンピュータに送信する通信制御部と、ホストコンピュータ側において、予め登録された暗証コードと指紋データと、受信した暗証コード及び指紋読取部の出力とを照合して本人確認を実行する本人確認処理部とを設けたことを特徴とする自動取引システム。

50 【0006】〈構成3〉自動取引装置側において、利用

者の指紋を読み取る指紋読取部と、利用者が投入したカードから、口座番号を読み取ってホストコンピュータに送信する通信制御部と、ホストコンピュータ側において、指紋データベースから上記口座番号に対応させて格納した指紋データを読み出して、利用者端末側に返送する指紋データベース検索部と、自動取引装置側において、返送された指紋データと、上記指紋読取部により読み取った指紋とを照合して、本人確認を行う照合部とを備えたことを特徴とする自動取引システム。

【0007】〈構成4〉構成3において、通信制御部は、利用者が入力した暗証コードと取引データとをホストコンピュータに送信し、ホストコンピュータ側において、自動取引装置側で指紋照合の結果本人と確認されると、暗証コードを利用して更に本人確認を行うとともに、取引データを使用して取引を実行して自動取引装置側に通知する制御部を備えたことを特徴とする自動取引システム。

【0008】〈構成5〉自動取引装置側において、利用者の指紋を読み取る指紋読取部と、利用者が投入したカードから口座番号を読み取って、利用者が入力した暗証コードと共にホストコンピュータに送信する通信制御部と、ホストコンピュータ側において、上記暗証コードを利用して本人確認を行い、本人と判断されたとき、指紋データベースから上記口座番号に対応させて格納した指紋データを読み出して、利用者端末側に返送する指紋データベース検索部と、自動取引装置側において、返送された指紋データと、上記指紋読取部により読み取った指紋とを照合して、本人確認を行う照合部とを備えたことを特徴とする自動取引システム。

【0009】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。

〈具体例1〉図1は、具体例1の装置のブロック図である。図の自動取引装置1は銀行等の金融機関に設置されているもので、カード出入口3、通帳出入口4、現金出入口5、操作パネル6等を備えている。更に、この具体例では、自動取引装置1の前面パネルに指紋スキャナ7を設けている。また、自動取引装置1は、利用者2が金融機関等において預貯金の入出金取引等に利用する装置である。なお、この装置をこの具体例では、例えば年金支給等に利用するものとする。

【0010】自動取引装置1の内部には、利用者2が投入したカード9からその中に格納されたデータを読み取るカード読取部11と、指紋スキャナ7の出力側に接続された指紋読取部12と、照合部13、取引制御部14等が設けられている。カード9は、例えばICカードから構成され、集積化されたメモリが埋め込まれている。この中に、予め登録された利用者2の指紋データが格納されている。カード読取部11は、カード9を装着してそのメモリの記憶領域をアクセスし、指紋データを読み

取る機能を持つ部分である。指紋スキャナ7は、利用者2が該当する指や掌を乗せた場合に、そのイメージデータを読み取り、所定のデータ処理を行って指紋データを得る部分である。指紋データの取得方法は従来よりよく知られており、詳細な説明は省略するが、指紋データの内容は、特定の1本あるいは複数本の指や掌の紋様を適当な方向に走査して得た陰影に対応するデジタル符号化データである。

【0011】照合部13は、カード読取部11と指紋読取部12の出力を受け入れて、それぞれから入力する指紋データを比較し、その一致度を結果として出力する部分である。取引制御部14は、照合部13が指紋データ照合の結果、利用者2をカード9の所有者本人と認識した場合に取引を開始する。その取引の内容は、例えば利用者2に対し該当する年金を支給するといった内容となる。なお、本人確認処理が終了した後は、利用者2は操作パネル6を操作して年金支給等の取引を実行する。取引制御部14は、ホストコンピュータ20と接続されており、ホストコンピュータ20に格納された取引用データベースを検索して、利用者2に対する取引の内容を確認し、所定の動作を行う。

【0012】顧客は年金支給を受けようとする場合、まず、カード9を自動取引装置1のカード出入口3に投入する。そして、指紋スキャナ7に指定された指を押し付ける。これによって、指紋スキャナ7は、利用者2の指紋を取得する。指紋読取部12は、取得した指紋から指紋データを生成する。自動取引装置1に投入されたカードは、カード読取部11にセットされる。そして、カード9のメモリ9Aから予め登録された指紋データが読み取られる。カード読取部11の出力と指紋読取部12の出力は照合部13に送り込まれ、指紋データの照合が行われる。照合結果が一致すれば、利用者2はカード9の所有者本人と確認される。そして、取引制御部14が年金支給の取引を開始する。もし、指紋データが一致しない場合には、年金支給の取引は拒絶される。

【0013】〈具体例1の効果〉この具体例1によれば、顧客が投入したカードに登録された指紋データと顧客自身の指から採取した指紋データとを照合してその結果に基づいて年金支給等の取引を実行するため、顧客がカードの所有者本人であることを確実に認識できる。従って、具体例1は、本人以外の者に対して取引を認めない各種の取引について自動取引装置1を安全確実に動作させるために広く利用することができる。

【0014】〈具体例2〉図2は、具体例2のシステムブロック図である。図のシステムは、自動取引装置1が通信回線10を介してホストコンピュータ20と接続されており、ホストコンピュータ20の側で本人確認を行う構成となっている。自動取引装置1には、具体例1の場合と同様に、操作パネル6と共に指紋スキャナ7が設けられている。指紋スキャナ7の出力は指紋読取部12

を介して通信制御部15に入力するよう構成されている。一方、ホストコンピュータ20には、制御部21、取引用データベース22、指紋データベース23、本人確認処理部24、暗証コード保持部25、指紋照合部26及び通信制御部27が設けられている。通信制御部27は、通信回線10を介して自動取引装置1の通信制御部15と接続される一方、指紋データ登録装置30と接続されている。ホストコンピュータ20は制御部21によって制御される。ホストコンピュータ20には、取引用データベース22を備えており、ここに銀行の預貯金データや年金支給データ等、各種のデータが格納されている。

【0015】指紋データベース23は、ホストコンピュータ20に対し通信回線10を介して接続されたいずれかの自動取引装置を用いて年金支給処理を行う利用者の指紋が予め登録されている。この指紋登録処理は、例えば各所に配置された指紋データ登録装置30等によって行われる。指紋データ登録装置30は、利用者の指や掌のイメージを予め取得して所定の指紋データを生成し、通信回線10を介してホストコンピュータ20に送り込む装置である。暗証コード保持部25は、利用者が自動取引装置1を使用して入力した暗証コードを一次的に格納し、本人確認のために利用するためのメモリである。本人確認処理部24や指紋照合部26は次のようにして動作し、利用者2が年金支給を受ける本人であることを確認する。

【0016】この具体例2は、利用者2がカード等を所持しない場合にも、本人確認を行うことができるようにしたものである。まず、利用者2が自動取引装置1を操作して、先に説明した通りの要領で指紋の読み取り操作を行う。更に利用者2は、操作パネル6を使用して暗証コードを入力する。指紋読取部12は、取得した指紋のイメージデータから所定の指紋データを生成し、通信制御部15に送り込む。また、利用者2が入力した暗証コードも通信制御部15に送り込まれる。そして、指紋コードと暗証コードは、通信回線10を介してホストコンピュータ20の通信制御部27に入力する。

【0017】ホストコンピュータ20では、暗証コードを暗証コード保持部25に記憶する一方、指紋照合部26が指紋データを受信し、指紋データベース23を検索して、一致する指紋データを見つける。なお、指紋データベース23に多数の指紋データが格納されている場合、その全てを参照して照合するのは処理時間が長時間になるおそれがある。そこで、例えば、各指紋データを暗証コードと対応させて格納しておき、暗証コード保持部25に格納された暗証コードをキーにして、照合対象となる指紋データを絞り込む。たとえ、同一の暗証コードを使用している利用者がいたとしてもごく僅かであるから、照合対象が絞られ、迅速に指紋データの照合ができる。こうして指紋データベース23から、指紋データ

と共に格納しておいた他の本人確認用のデータを取り出し、これを本人確認処理部24に送り込む。本人確認処理部24は、取引用データベース22を参照して、該当する利用者のデータを読み取り、暗証コードその他を照合した上で本人であるとの確認を行う。このような確認処理が終了すると、必要な取引データと共にホストコンピュータ20から応答が自動取引装置1の側に送信される。これによって、自動取引装置1において、利用者2に対する年金支給処理等が開始される。もし、本人であると認識されなかった場合には、年金取引は拒絶される。

【0018】〈具体例2の効果〉指紋の照合のみならず、暗証コードの入力によって更に精度の高い本人確認処理を行い、年金支給取引等の取引に対する安全性を確保できる。また、ホスト側に指紋データベースを保存しておくため、指紋データベースの安全性、確実性が増す。なお、予め利用者2が年金支給取引を開始するという意志と、暗証コードを入力することによって、一旦年金支給対象者に該当するかどうかの選別を行った後、指紋データの照合を行うといった手順を採用すれば、ホスト側において無駄な指紋照合処理を排除することもできる。しかも、利用者はカードを必要とせず、簡便な取引が可能となる。

【0019】〈具体例3〉図3は、具体例3のシステムのブロック図である。この装置は、指紋の照合を自動取引装置側において行う。一方、指紋データベースはホストコンピュータ側に設けられている。そこで、口座番号をもとに指紋データをホストコンピュータ側から自動取引装置側に転送し、指紋の照合を行う。

【0020】具体的にはこのシステムは、ホストコンピュータ20の側に、制御部21、取引用データベース22、指紋データベース23、指紋データベース検索部29及び通信制御部27を設ける。また、自動取引装置1の側には、カード読取部11、指紋読取部12、照合部13、通信制御部15及び取引制御部16を設ける。ホストコンピュータ20の側の制御部21、取引用データベース22、指紋データベース23及び通信制御部27等の構成は、具体例2で説明したものとほぼ同様である。なお、指紋データベース23は、この例では口座番号に対応させて指紋データを格納した構造となっている。即ち、各口座番号に該当する口座を所有する利用者の指紋データが、口座番号に対応して格納されている。指紋データベース検索部29は、自動取引装置から受け付けた口座番号をもとに、指紋データベース23を検索して該当する指紋データを得る部分である。なお、この指紋データは、通信制御部27を介して自動取引装置側に返信される構成となっている。

【0021】自動取引装置1の側に設けられたカード読取部11は、利用者2がカード出入口3から投入したカードの磁気ストライプを読み取って口座番号を得る装置

である。この口座番号は通信制御部15を介してホストコンピュータ20の側に送られる。また、指紋読取部12の構成や動作はこれまで説明したものと同様である。その読取結果は照合部13に送られる。照合部13は、通信制御部15を介してホストコンピュータ20から送り込まれた指紋データと指紋読取部12の出力とを照合して利用者2がカード9の所有者本人かどうかの確認を行う部分である。その確認結果は取引制御部16に向けて出力される。取引制御部16は、利用者2の操作に従って受け入れた暗証コードや取引データを通信制御部15を介してホストコンピュータ20に送信する構成となっている。この取引データは、ホストコンピュータ20の側に受信され、制御部21が取引用データベース22を参照しながら所定の取引を実行するように構成されている。

【0022】以下、このシステムの動作を更に具体的に説明する。まず、利用者2が自動取引装置1の操作パネル6を操作して取引の種類を選択する。次に、利用者2は、カード9をカード出入口3に投入する。カード読取部11はカード9から口座番号を読み取って、通信制御部15を介してホストコンピュータ20に転送する。なお、通信回線10を転送される各信号は、それぞれS1～S4というように送受信される順番に符号を付けた。ホストコンピュータ20の側では、口座番号を受信すると、指紋データベース検索部29が指紋データベース23を参照して口座番号に対応する指紋データを読み取る。この指紋データは通信制御部27を介して自動取引装置の側に返送される。照合部13はこの指紋データを受信する。ホストコンピュータ20から指紋データが転送されてくると、指紋読取部12の制御によって、操作パネル6に利用者2に対し指紋採取を要求するメッセージを表示する。利用者2は、指紋スキャナ7の上に指や掌を乗せる。指紋読取部12は、こうして利用者2の指紋を読み取る。その出力は照合部13に送られる。照合部13は、指紋読取部12の出力とホストコンピュータ20から転送された指紋データとを比較照合して利用者2がカード9を保持している本人かどうかを判断する。

【0023】なお、カード9に記録された口座番号が実際には存在しないような番号である場合には、指紋データベース23から該当する指紋データを読み出すことができない。従って、こうした場合には照合部13の動作を待たずに利用者2に対し取引ができない旨の通知がされる。一方、照合部13において、利用者2がカード9の所有者本人と判断されると、その結果が取引制御部16に通知され、利用者2による各種の取引データの入力が進められる。入力が終わった取引データは、利用者が入力した暗証コードと共に再び通信制御部15を介してホストコンピュータ20に送信される。ホストコンピュータ20の制御部21はこの取引データを受信し、暗証コードの照合を行ってから、取引用データベース22を参

照しながら一定の取引処理を実行する。そして、取引が正常に終了すると、自動取引装置に対し取引結果が通知される。この結果は取引制御部16を介して操作パネル6に表示され、取引が終了する。

【0024】〈具体例3の効果〉以上の構成によれば、指紋データベース23をホストコンピュータ20の側に保存するため、指紋データの集中管理が可能となる。また、指紋照合は自動取引装置の側において行うため、ホストコンピュータの負担が軽減される。更に、口座番号に対応する指紋データと実際に利用者から取得した指紋との照合を行うことから、指紋データベースにある全ての指紋データとの照合を行う場合に比べて照合処理が短時間に行われる。これらの他に、取引を開始して、更に利用者2から暗証コードの入力を受け、制御部21において暗証コードを用いた取引用データベース22の参照を実行すれば、指紋データの照合に更に暗証コードの照合という処理が行われるため、一層セキュリティが高まる。指紋照合のみとするか暗証コードの照合も合わせて行うかは、要求されるセキュリティに応じて決めればよい。

【0025】〈具体例4〉図4には、具体例4のシステムのブロック図を示す。具体例3では、指紋照合による本人確認を自動取引装置の側で行い、必要に応じて更にホストコンピュータ20の側でも暗証コードを用いた本人確認を行うようにした。この暗証コードによる本人確認は、指紋照合による本人確認よりも先に行うようにしても構わない。この具体例4は、その趣旨から構成されたシステムである。

【0026】ホストコンピュータ20の側には、制御部21、取引用データベース22、指紋データベース23、本人確認処理部24、指紋データベース検索部29及び通信制御部27が設けられている。この本人確認処理部24以外の部分は、図3に示した具体例3のホストコンピュータの構成と変わるところはない。この本人確認処理部24は、後で説明する要領で、自動取引装置側から受信された口座番号と暗証コードを用いて取引用データベース22を参照し、まず本人確認を行う。そして、本人であると確認すると、その結果を指紋データベース検索部29に通知する構成となっている。指紋データベース検索部29は本人確認処理部24の通知を受けた後、指紋データベース23を検索して、口座番号に対応する指紋データを読み取り、自動取引装置側に送信する構成となっている。また、自動取引装置1の側には、図3と同様のカード読取部11、指紋読取部12、照合部13、通信制御部15及び取引制御部16が設けられている。

【0027】以上の構成のシステムは、次のように動作する。まず、利用者2がこれまでと同様に操作パネル6を操作して、取引の種類を選択する。そして、次に、カード9をカード出入口3に投入すると、カード読取部1

1は、カード9の磁気ストライプから口座番号を読み取り、通信制御部15を介してホストコンピュータ20に送信する。一方、取引制御部16が操作パネル6に暗証コードの入力を要求する表示を行う。利用者2は、これに対応して操作パネル6を操作し、暗証コードを入力する。この暗証コードも通信制御部15を介してホストコンピュータ20に送信される。ホストコンピュータ20の側では、口座番号と暗証コードを受信すると、本人確認処理部24がこれを受け入れて、取引用データベース22を参照する。これによって、該当する口座番号の該当する暗証コードで正規の利用者が存在するかを判断する。

【0028】こうして、暗証コードを用いた本人確認処理が行われると、その結果が指紋データベース検索部29に送られる。指紋データベース検索部29は暗証コードによる本人確認によって本人と判断された場合のみ指紋データベース23から口座番号に対応する指紋データを読み出す。そして、指紋データは通信制御部27を介して自動取引装置の側に送信される。この指紋データは自動取引装置1の側において、照合部13に受け入れられる。指紋読取部12は、これまで説明したと同様の手順で利用者2から指紋を読み取り、照合部13に向け出力する。照合部13は利用者2の指紋とホストコンピュータの側から送信された指紋データとを照合し、本人と確認されると、取引制御部16にその旨を通知する。これによって、取引制御部16は利用者2の取引を受け入れて、その後取引を実行する。

【0029】〈具体例4の効果〉以上の処理によれば、具体例3と同様に、指紋データベースをホストコンピュータ20の側に持つことができる。また、自動取引装置の側で指紋照合による本人確認を実行することができる。一方、この具体例では、予め口座番号と暗証コードを用いてホストコンピュータの側で本人確認を行い、本人と確認された場合にのみ指紋データベースから該当する指紋データを検索し、自動取引装置の側に送る。従って、暗証コードによって取引が拒否された場合には、その後の指紋照合等の処理を必要とせず、操作が簡略化される。また、指紋データはほぼ本人に間違いのないような場合にのみ、通信回線10を介して送信されることから、通信回線10のトラフィック減少に役立つ。

【図面の簡単な説明】

【図1】具体例1の装置のブロック図である。

【図2】具体例2のシステムブロック図である。

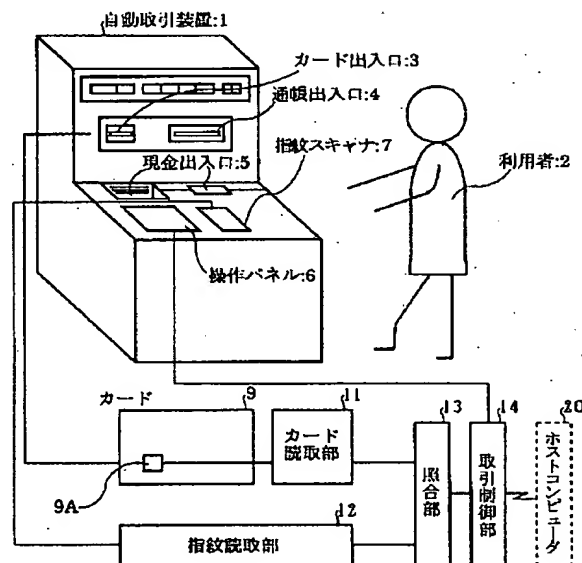
【図3】具体例3のシステムのブロック図である。

【図4】具体例4のシステムのブロック図である。

【符号の説明】

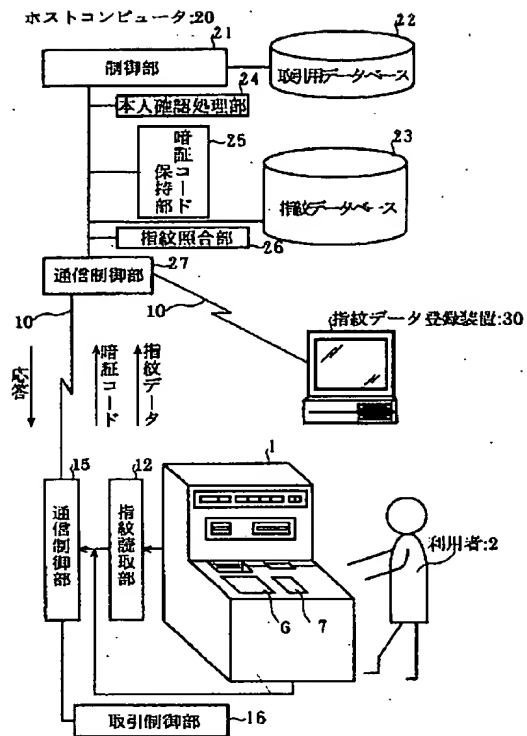
- 1 自動取引装置
- 2 利用者
- 7 指紋スキャナ
- 9 カード
- 11 カード読取部
- 12 指紋読取部
- 13 照合部

【図1】



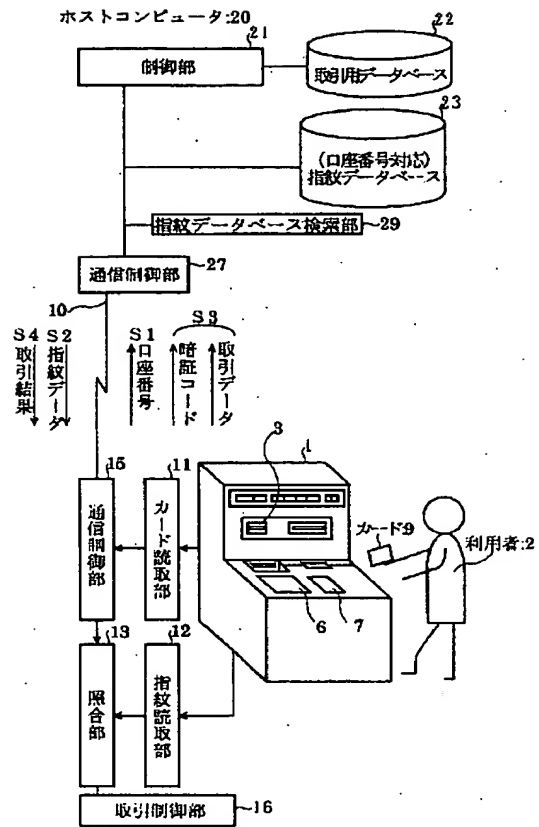
具体例1のシステムのブロック図

【図2】



具体例2のシステムのブロック図

【図3】



具体例3のシステムのブロック図

